

CITY OF SAN ANTONIO



Administrative Directive	AD 7.8A Information Security Directive Summary
Procedural Guidelines	Guidelines that establish directives for the security of information assets.
Department/Division	Information Technology Services Department (ITSD)
Effective Date	July 6, 2009
Project Manager	John Byers, Chief Information Security Officer (CISO)

Purpose

The purpose of this directive is to establish responsibility and provide general guidance for all of Information Technology Services Department (ITSD) and City of San Antonio (COSA) employees for the protection of information resources entrusted to each person in the performance of City's business.

Policy

This directive provides a mechanism to establish procedures to protect against security threats and minimize the impact of security incidents.

Policy Applies To

<input type="checkbox"/> External & Internal Applicants	<input checked="" type="checkbox"/> Current Temporary Employees
<input checked="" type="checkbox"/> Current Full-Time Employees	<input type="checkbox"/> Current Volunteers
<input checked="" type="checkbox"/> Current Part-Time Employees	<input checked="" type="checkbox"/> Current Grant-Funded Employees
<input checked="" type="checkbox"/> Current Paid and Unpaid Interns	<input checked="" type="checkbox"/> Police and Fire Academy Trainees
<input checked="" type="checkbox"/> Uniformed Employees Under Collective Bargaining Agreements	

Definitions

Policy Guidelines

General Guidelines

- A. For the purpose of this directive and other information security directives, information systems or information technology includes, but is not limited to:

1. Transaction processing systems
 2. Decision support systems
 3. Knowledge management systems
 4. Database management systems
 5. Office information systems
 6. Communications systems (e.g., networks, phones, wired, wireless, and other forms of data communications, and voice/media communications methods and processes)
- B. Information and associated computer resources are vital assets requiring protection appropriate to their value. Measures shall be taken to protect information assets against accidental or unauthorized disclosure, modification, or destruction in order to ensure their availability, integrity, reliability, and confidentiality.
- C. Specific standards, procedures, and guidelines issued in support of this directive will be communicated to all employees and will be used as a basis for compliance monitoring and review. Security directives, both physical security and information security, are developed to provide information, instruction, and guidance to protect and safeguard COSA resources.
- D. The Alliance for Telecommunications Industry Solutions (ATIS) defines an "information system" as "a system, whether automated or manual, that comprises people, machines, and/or methods organized to collect, process, transmit, and disseminate data that represent user information." This includes, "any telecommunications and/or computer related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data, and includes software, firmware, and hardware" (ATIS Telecom Glossary 2007)
- E. Guidance for requesting exceptions to or deviations from this directive is outlined in *AD 7.5A Establishing IT-Related Directives*

Roles & Responsibilities

Chief Information Security Officer

- A. Review this directive annually, at a minimum, for both consistency and accuracy
- B. Interpret and apply this directive under the direction of the Chief Information Officer (CIO) and/or the Chief Technology Officer (CTO), as appropriate
- C. Modify or amend this directive at any time pending formal review and approval as defined in *AD 7.5A Establishing IT-Related Directives*

	D. Provide adequate notice of any such modifications or amendments E. Ensure the current version of this directive is posted in a public location accessible to all authorized City personnel
<u>Departments</u>	A. Responsible for any disciplinary action taken against employees who violate this directive
<u>Human Resources</u>	A. Provide guidance, as required, to City departments regarding appropriate disciplinary action to be taken against employees who violate this directive
<u>Attachments</u>	
<u>N/A</u>	


Information and/or clarification may be obtained by contacting the Information Technology Services Department (ITSD) at 207-8301.



 Hugh Miller
 Information Technology Services Department Director / CTO

09/14/2009

 Date

Approved by:


 Richard J. Varn
 Chief Information Officer (CIO)

09/16/2009

 Date

Approved by:


 Sheryl Sculley
 City Manager

9-29-09

 Date